

«КриптоАРМ» версии 5.3



Краткое руководство пользователя

Содержание руководства



Что такое «КриптоАРМ»	3
Установка «КриптоАРМ»	4
Установка лицензии	5
Установка сертификатов с токена или смарт-карты	7
Установка сертификатов с дискеты или флешки	16
Управление профилями	17
Как подписать файл	23
Как добавить подпись	26
Как проверить подпись	28
Как зашифровать файл	39
Как расшифровать файл	32
Как просмотреть документ	34
Техническая поддержка	35

Что такое “КриптоАРМ”?



КриптоАРМ - программа для шифрования и электронной подписи файлов любого формата и размера (в т.ч. PDF, DOCX, XLSX, JPG, PNG).

Программа соответствует всем требованиям российского законодательства в части обеспечения юридически значимого статуса и используется для подписания котировочных заявок, банковских гарантий, межевых планов, алкогольных деклараций, различных соглашений, договоров, контрактов и других документов.

Используется в информационных системах, в которых необходимо:

- надежно защитить данные от постороннего доступа;
- обеспечить подлинность и авторство электронных документов;
- согласовывать электронные документы с коллегами;
- гарантировать целостность данных при отправке по незащищенным каналам связи и т.д.

Установка «КриптоАРМ»



1. Скачать дистрибутив

Актуальная версия программы: www.trusted.ru/support/downloads/

2. Убедиться в наличии прав администратора

Установка программы «КриптоАРМ» без наличия прав невозможна.

3. Установить программу

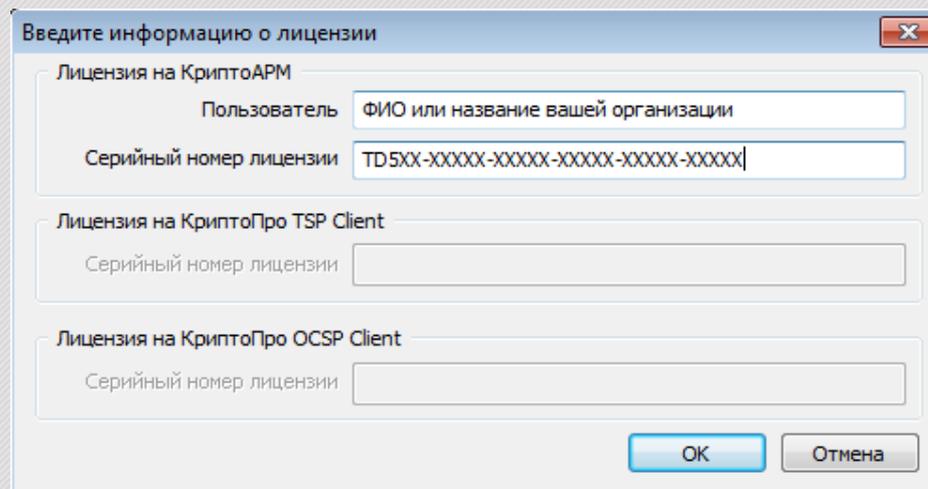
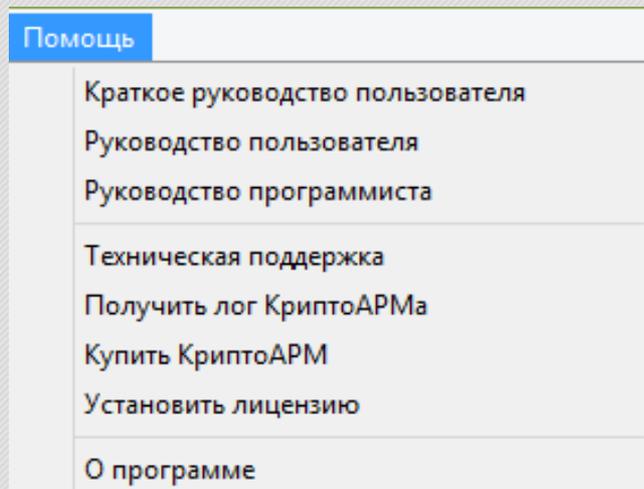
При первичной установке программы на компьютер автоматически будет активирован 30-дневный ознакомительный период «КриптоАРМ Стандарт Плюс» или «КриптоАРМ Терминал» (в зависимости от типа операционной системы). По истечению ознакомительного периода программа автоматически переключится в режим «КриптоАРМ Старт» и предложит приобрести лицензию в официальном интернет-магазине:

<http://cryptoarm.ru/>

Установка лицензии



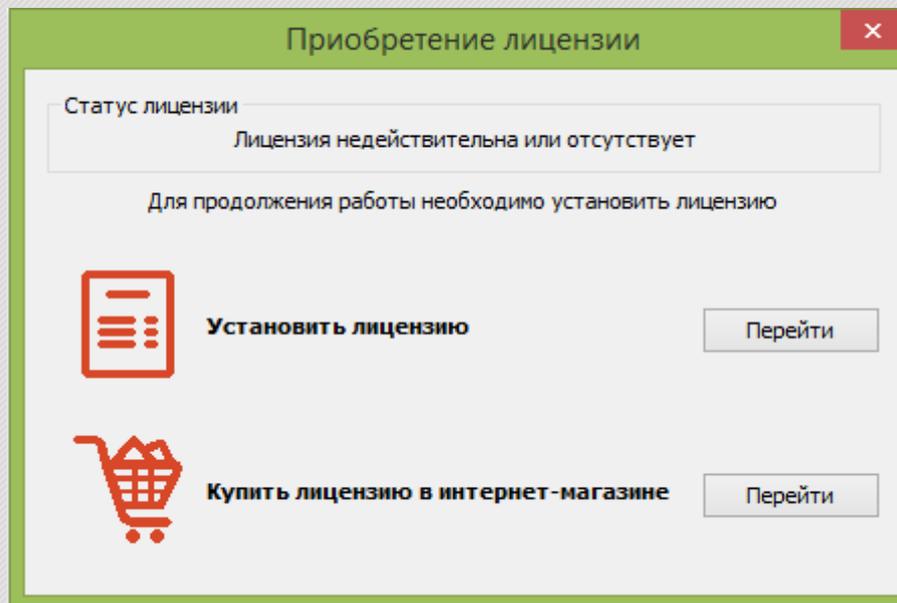
Вариант 1: Для установки лицензии зайдите в раздел **Помощь - Установить лицензию**, введите название вашей организации и серийный номер лицензии.



Установка лицензии



Вариант 2: Если ознакомительный период уже истек, то после каждого запуска программы вам будет предложено окно для удобной покупки и установки лицензии.



Установка сертификатов с токенов или смарт-карт



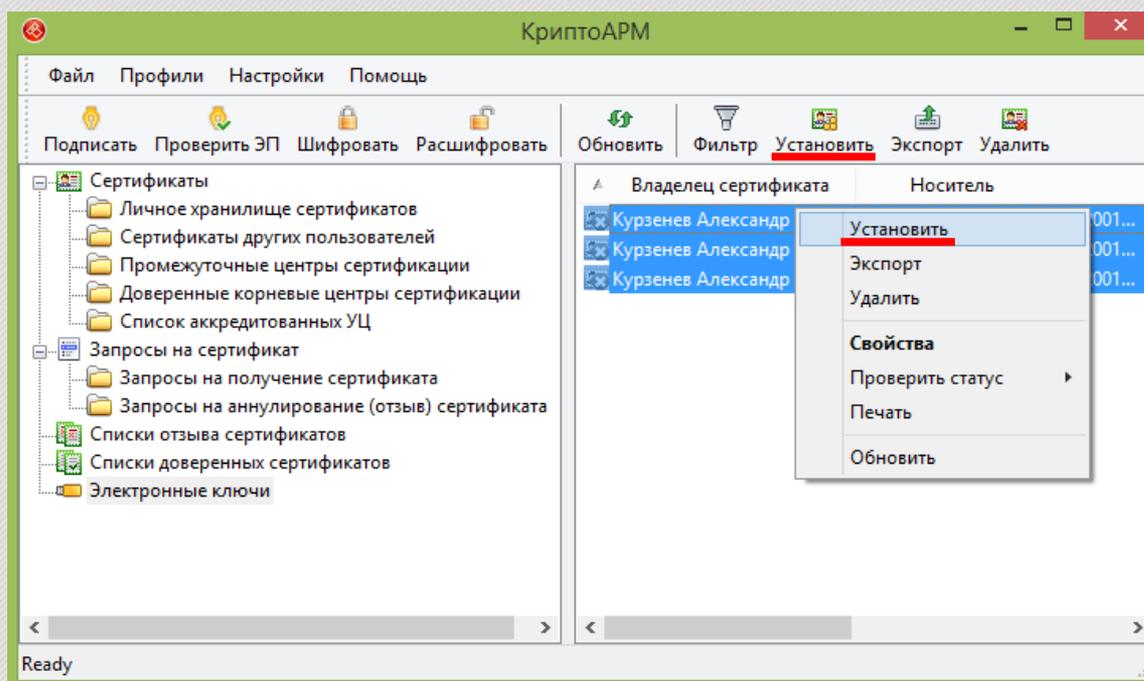
Для установки сертификата на компьютер необходимо:

1. Установить криптопровайдер (КриптоПро CSP) и соответствующий драйвер для ключевого носителя;
2. Подключить токен или смарт-карту к компьютеру (поддерживаются ключевые носители Рутокен, eToken, JaCarta, ESMART, Gemalto);
3. Зайти в ветку «Электронные ключи» и дождаться пока программа «КриптоАРМ» считывает все сертификаты, хранящиеся на токене или смарт-карте;
4. Неустановленные на компьютере сертификаты, хранящиеся на подключенных электронных ключах, будут отображены серым цветом (см. картинку ниже).

Установка сертификатов с токенов или смарт-карт



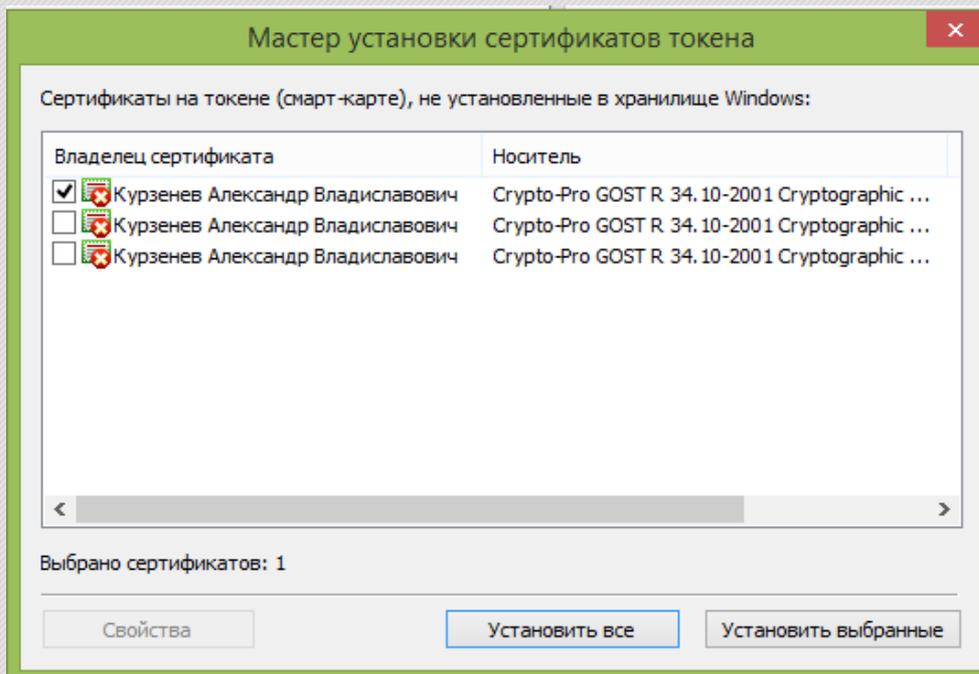
5. Выберите интересующие вас сертификаты и нажмите кнопку **Установить** на панели или в контекстном меню.



Установка сертификатов с токенов или смарт-карт



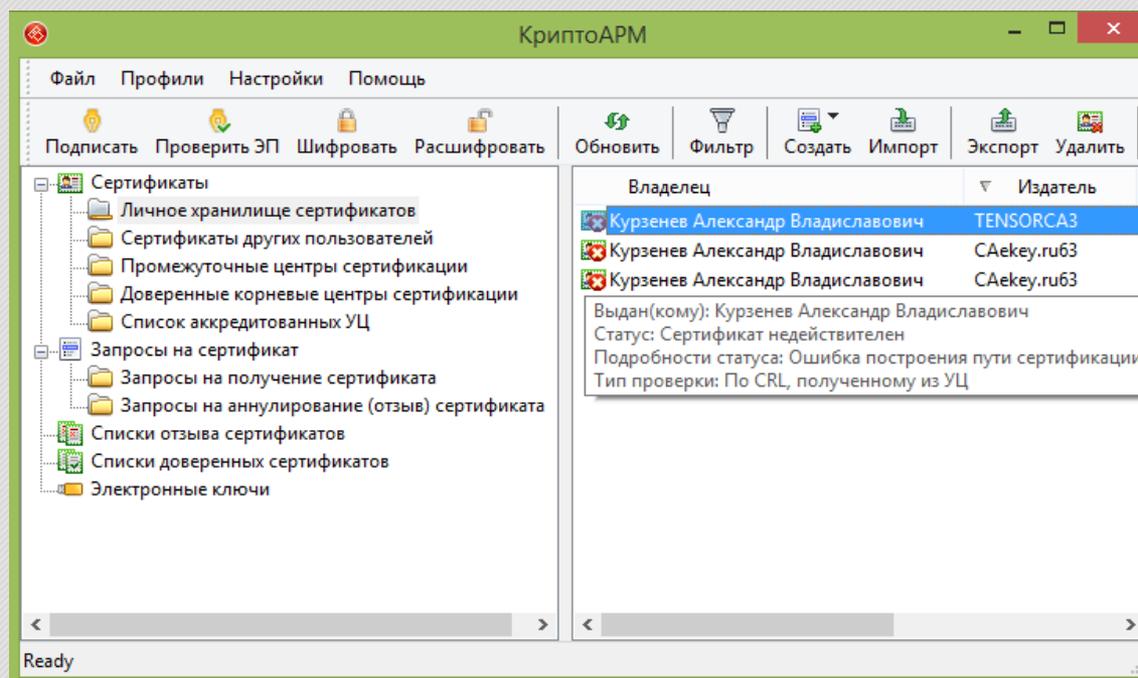
6. Выберите интересующие вас сертификаты и нажмите кнопку Установить выбранные или на кнопку Установить все.



Установка сертификатов с токенов или смарт-карт



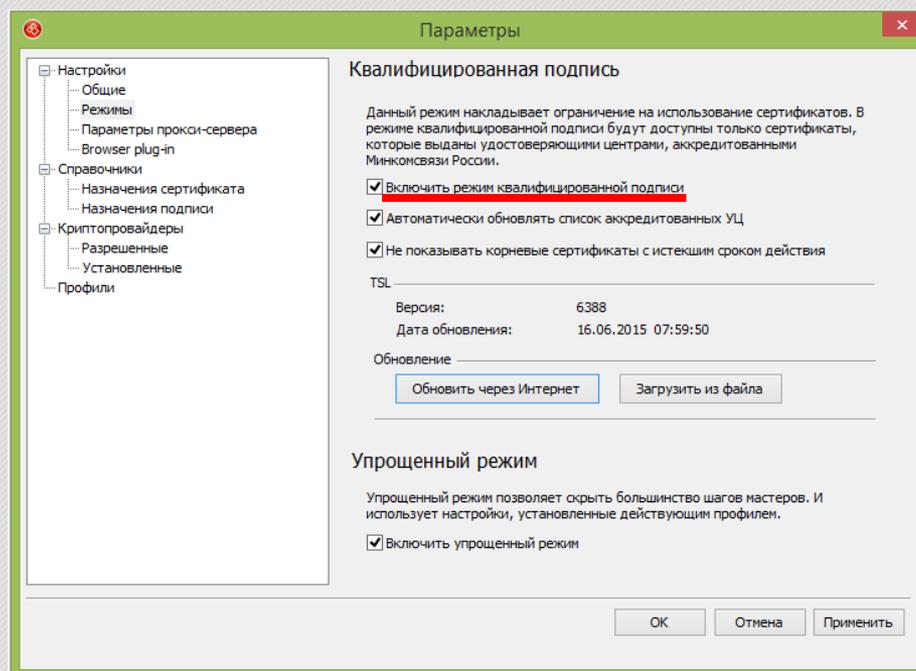
7. Ваши сертификаты будут установлены в Личное хранилище сертификатов со статусом «Ошибка построения пути сертификации»



Установка сертификатов с токенов или смарт-карт



8. Для автоматического построения пути сертификации в Настройках программы воспользуйтесь режимом Квалифицированная подпись.

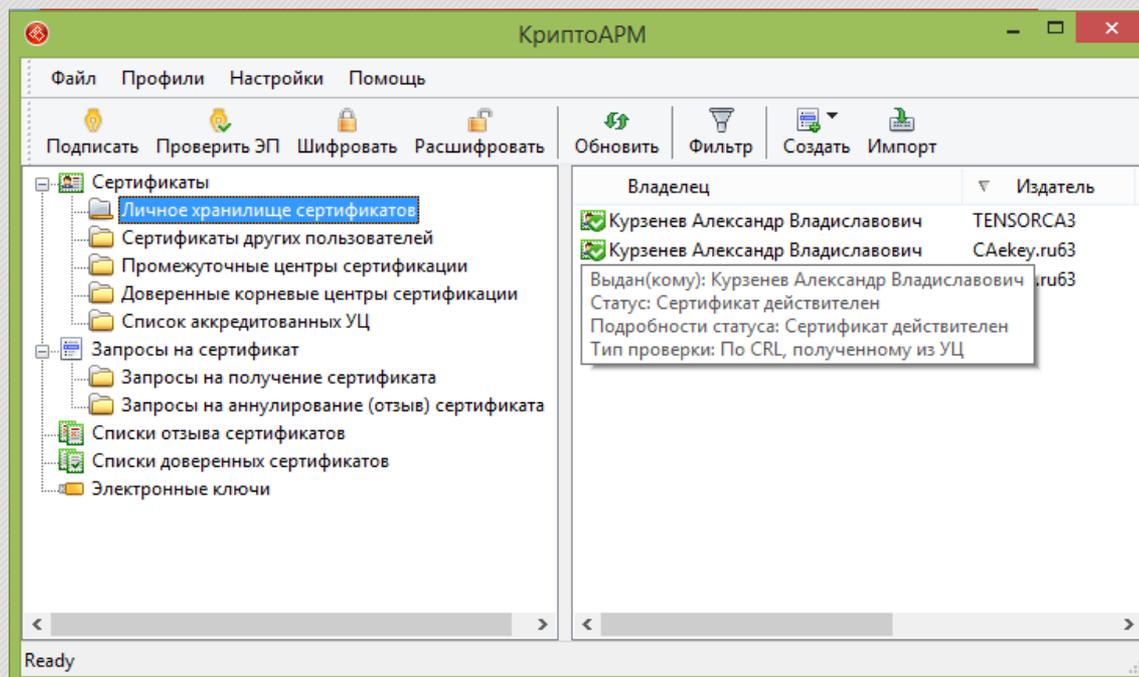


Примечание:
Данный режим предназначен только для квалифицированных сертификатов и требует наличия соединения с интернетом.

Установка сертификатов с токенов или смарт-карт



9. Поздравляем! Все необходимые сертификаты установлены!

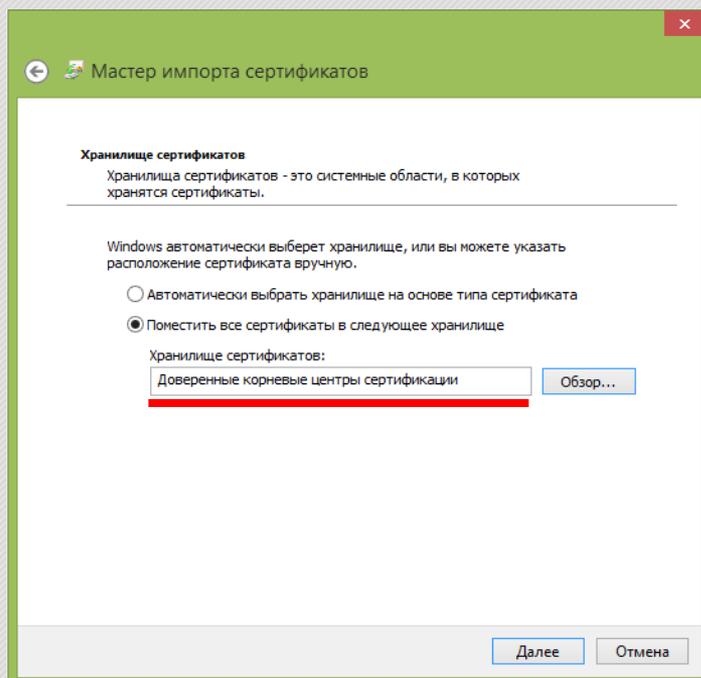


Если режим Квалифицированная подпись вам не помог, то отключите его и воспользуйтесь инструкцией для ручной установки необходимых сертификатов и списков отзыва сертификатов (шаги 10-13).

Установка сертификатов с токенов или смарт-карт



11. При установке корневого сертификата важно поместить его в хранилище Доверенные корневые центры сертификации

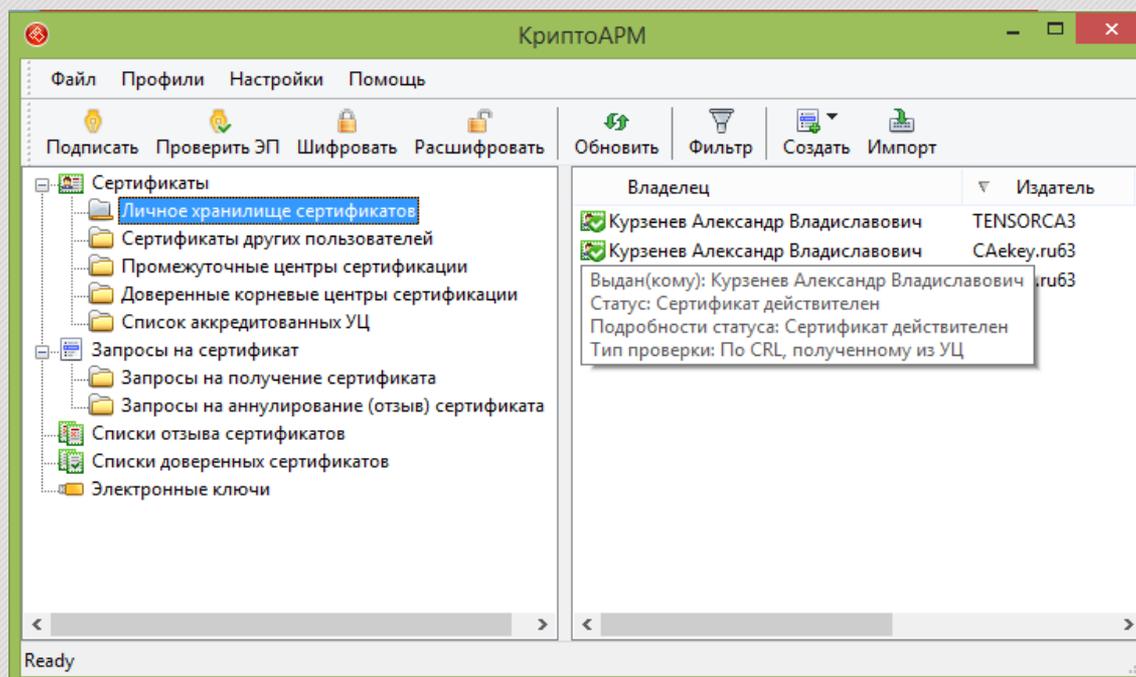


Примечание:
Важно принудительно выбрать именно данное хранилище. При автоматическом выборе хранилища возможна некорректная установка сертификата.

Установка сертификатов с токенов или смарт-карт



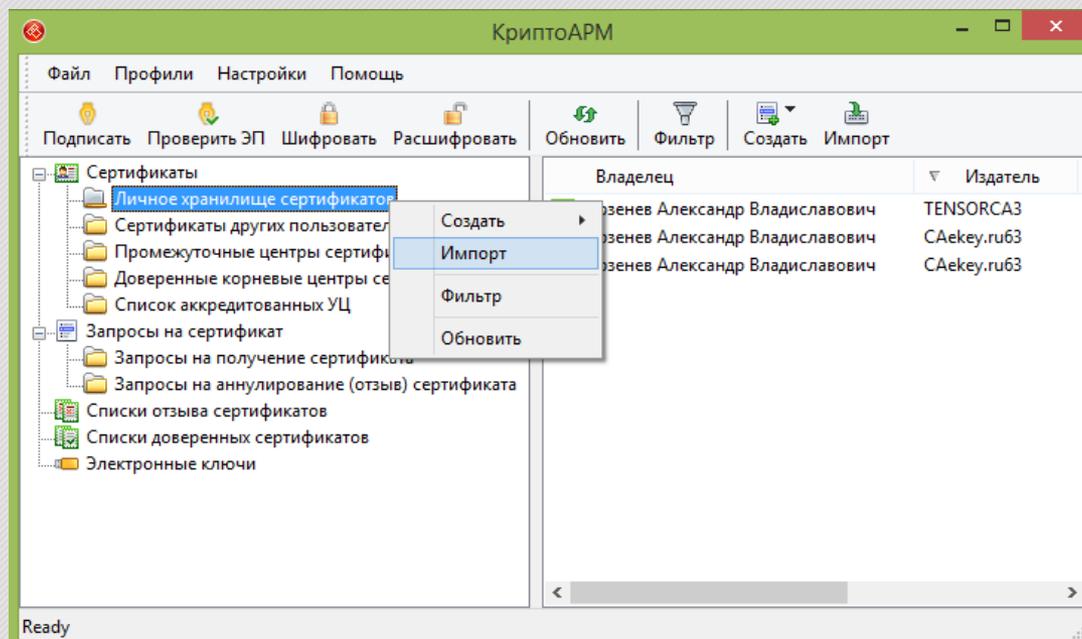
12. Поздравляем! Все необходимые сертификаты установлены!



Установка сертификатов с дискеты или флешки



Если ваш сертификат хранится на обычной дискете или флешке, то для установки сертификата необходимо воспользоваться мастером Установки сертификатов, CRL и CTL.

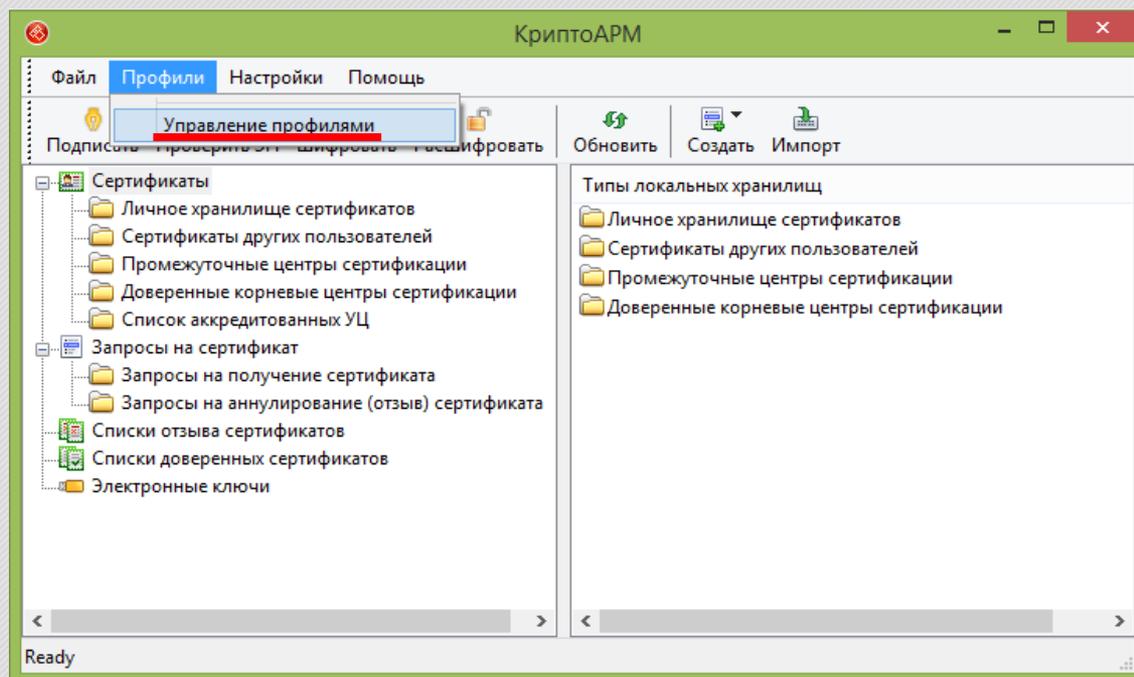


Внимание!
Мы не рекомендуем использовать незащищенные отчуждаемые носители, а также локальное хранилище для хранения закрытого ключа.

Управление профилями



Для упрощения работы с электронной подписью и шифрованием файлов вы можете использовать Профили, которые позволят сохранить необходимые настройки заранее.

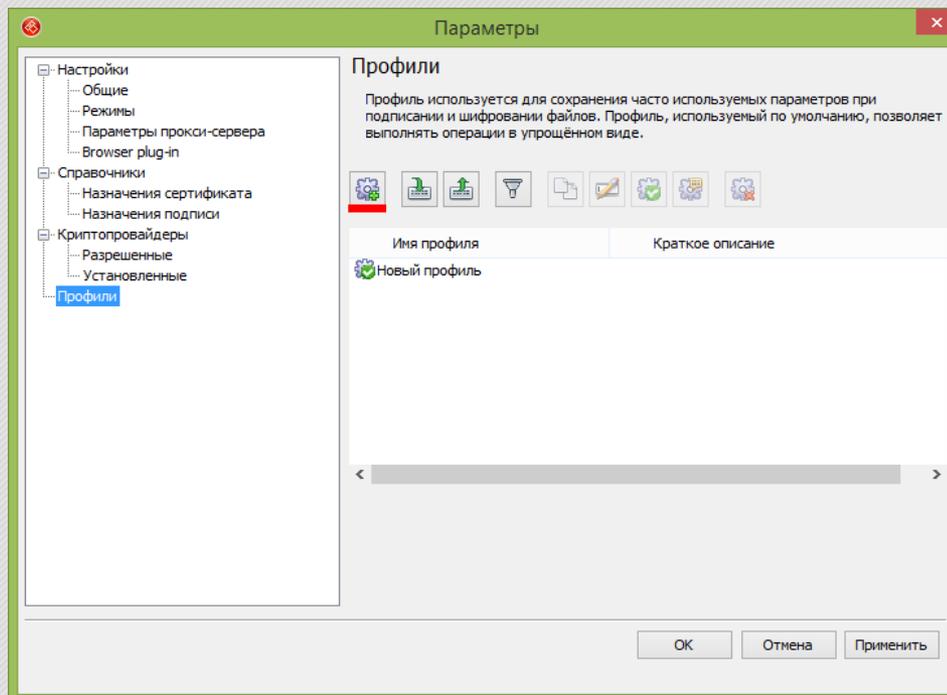


Для того, чтобы создать свой первый профиль, зайдите в раздел Управление профилями.

Управление профилями



Для того, чтобы создать новый профиль нажмите на кнопку Создать (левая кнопка на панели).



Кнопки на панели:

- Создать
- Импорт
- Экспорт
- Фильтр
- Создать копию
- Переименовать
- По умолчанию
- Свойства
- Удалить

Управление профилями



В разделе **Общие** введите имя профиля, а также выберите настройки, исходя из своих требований.

Обратите особое внимание на возможность добавить информацию о подписи с распечатываемый документ, а также выбрать сертификат из личного хранилища сертификатов.

Управление профилями



В разделах Подпись и Шифрование выберите настройки, исходя из своих требований. Обратите внимание на возможность сохранения подписи в отдельном файле и выбора расширения.

Параметры настройки

Профиль

- Общие
- Подпись**
- Шифрование
- Расшифрование
- Интерфейс пользователя
- Политика сертификатов
- Верификация сертификатов
- TSP
- OCSF
- Каталоги

Подпись

Параметры подписи

Тип хэш алгоритма: [Выбор]

Формат подписи: [Классическая]

Использование подписи: [Не задано]

Комментарий к подписи: [Поле]

Идентификатор ресурса: [Поле]

Помещать имя исходного файла в поле "Идентификатор ресурса"

Включать время создания подписи

Включать в подпись штамп времени на подпись на подписываемые данные

Включать в подпись: [Только сертификат владельца]

Сохранять подпись в отдельном файле

Удалять исходный файл после создания подписи

Выходной формат и расширение файла подписи

DER - кодировка *.sig BASE64 - кодировка *.sig

Включать архивирование Отключить служебные заголовки

Сохранять структуру вложенности каталогов

OK Отмена Применить

Параметры настройки

Профиль

- Общие
- Подпись
- Шифрование**
- Расшифрование
- Интерфейс пользователя
- Политика сертификатов
- Верификация сертификатов
- TSP
- OCSF
- Каталоги

Шифрование

Определение алгоритма шифрования

Криптопровайдер: Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service

Тип алгоритма шифрования: [GOST 28147-89]

Шифровать в адрес отправителя

Сертификаты получателей по умолчанию

Владелец	Издатель	Действителен с	Дейст
[Пустая таблица]			

[Просмотреть] Добавить... Удалить

Тип сообщения: [Классический (PKCS#7)]

Выходной формат и расширение зашифрованного файла

DER - кодировка *.enc BASE64 - кодировка *.enc

Отключить служебные заголовки

Удалить исходный файл после шифрования

Включить архивирование

Сохранять структуру вложенности каталогов

OK Отмена Применить

Управление профилями



В разделе Верификация сертификатов добавьте один, несколько или все сертификаты, для которых необходимо автоматическое обновление списков отзыва сертификатов. Нажмите кнопку ОК.

Параметры настройки

Верификация сертификатов

Сертификаты, для которых необходимо получение CRL из

Владелец	Издатель
<input checked="" type="checkbox"/> CN=Курзнев Александр ...	CN=TENSORCA3, O=ООО Компания ...

Добавить... Добавить все УЦ Удалить Удалить все

В данном списке для сертификатов, не отмеченных галочкой, CRL не будут загружаться из УЦ, если не выпущено новой версии.

Получение CRL из УЦ | Revocation Provider | Служба актуальных статусов (OCSP)

Использовать CTL для проверки пути сертификации

Проверять наличие подписи в CTL

Список доверия сертификатов: _____

Просмотреть Выбрать... Очистить

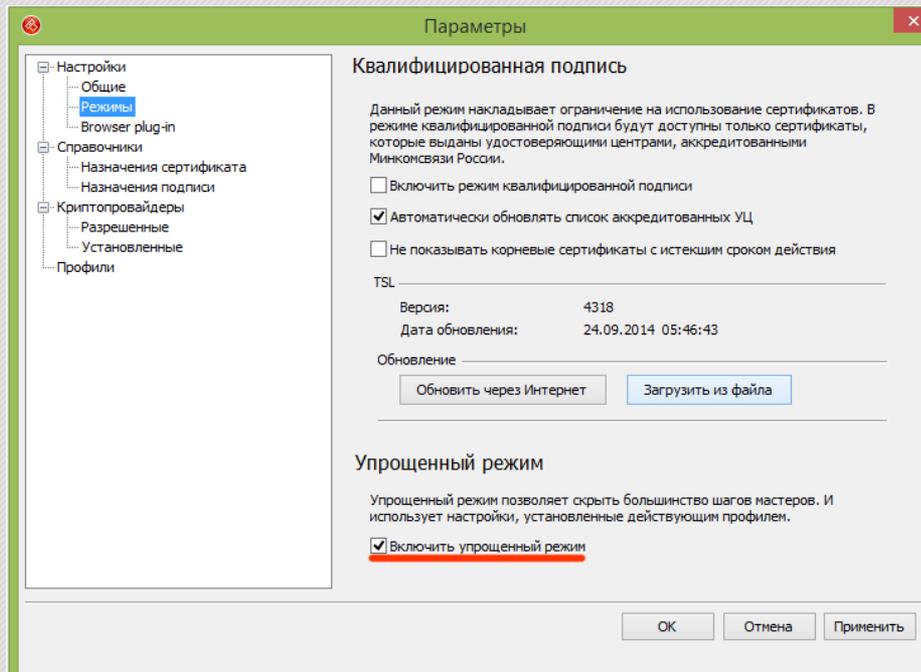
ОК Отмена Применить

Примечание:
После нажатия на кнопку ОК редактирование профиля завершится, настройки профиля сохранятся, и окно будет закрыто.

Управление профилями



После того, как вы выбрали все необходимые настройки профиля, нажмите **Применить**, а затем во вкладке **Режимы** включите **Упрощенный режим**.

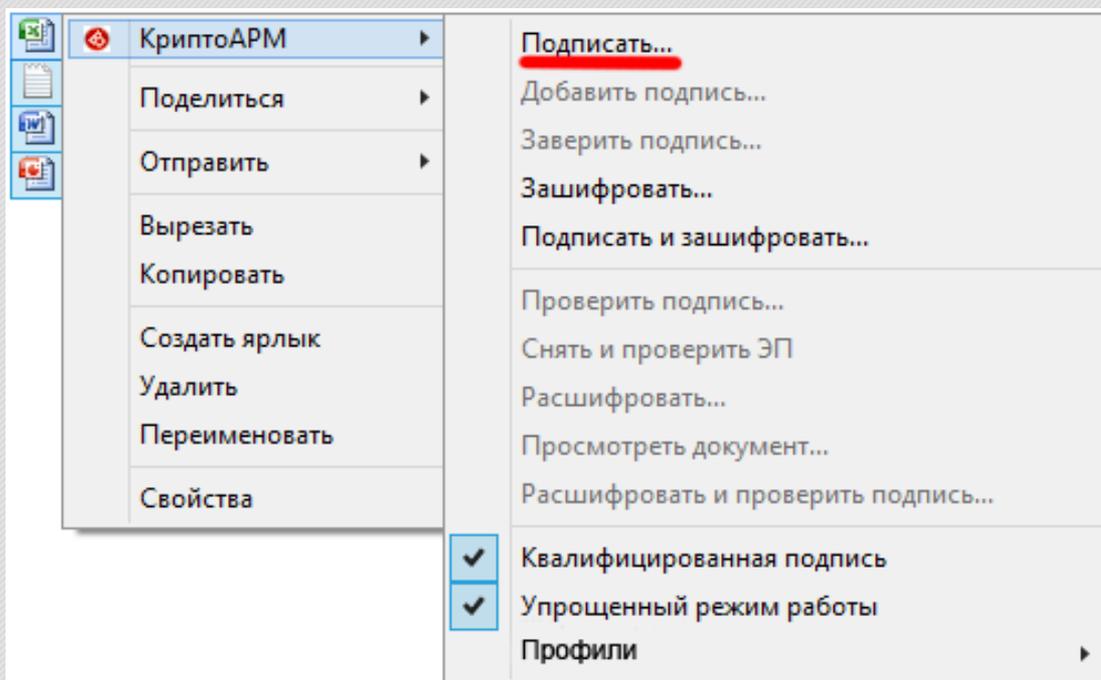
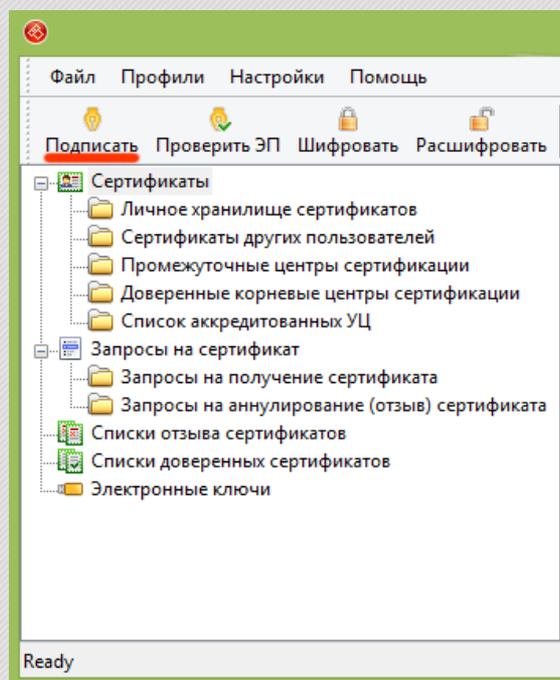


На этом настройка вашего профиля завершена. Далее рассмотрим операции подписания и шифрования уже с учетом включенного упрощенного режима.

Как подписать файл



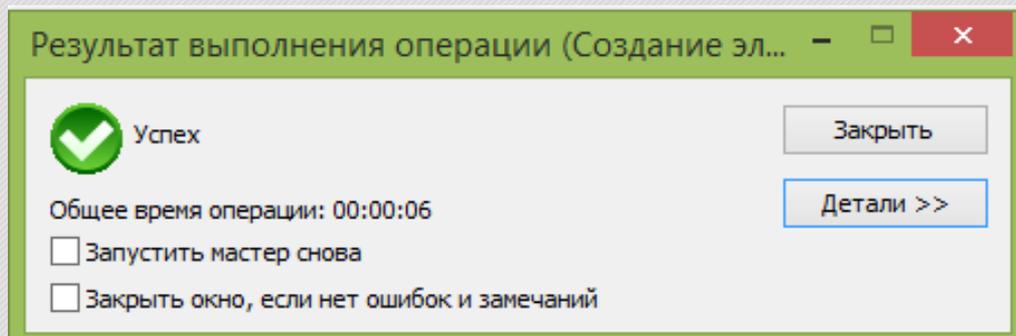
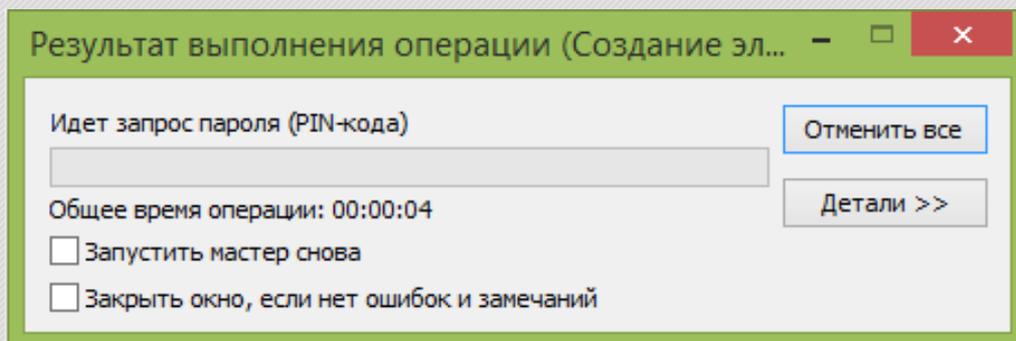
Подписать файлы можно в главном окне программы и через контекстное меню файла. Программа позволяет подписывать несколько файлов любого формата одновременно.



Как подписать файл



В зависимости от размера и количества файлов, а также от конфигурации рабочего места операция может занять от нескольких секунд до нескольких минут.



Обратите внимание, что данное окно появится сразу только при использовании сохраненного профиля и упрощенного режима (см. страницы 18-22).

Как подписать файл



В результате операции в той же папке, в которой хранился исходный документ, появится файл с аналогичным названием, но с расширением *.SIG

Если в профиле был включен параметр «Сохранять подпись в отдельном файле», то в результате вы получите отсоединенную подпись, которую необходимо отправлять вместе с исходным файлом.

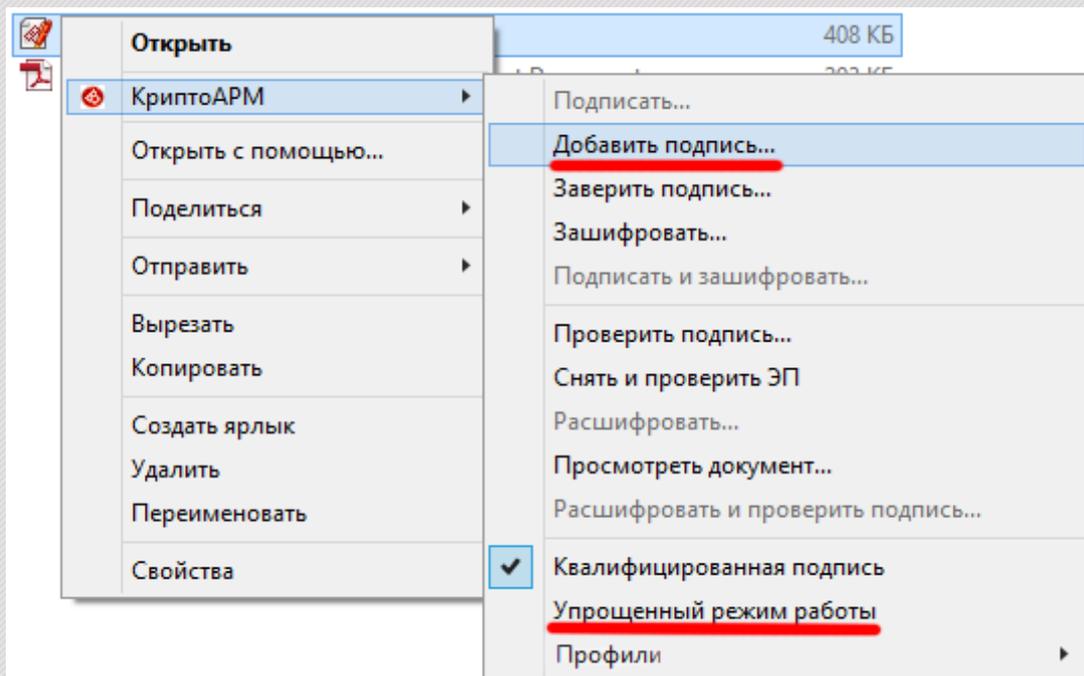
Имя	Тип	Размер
 Совмещенная	Документ Microsoft Office Word	30 КБ
 Совмещенная.docx	Файл "SIG"	<u>46 КБ</u>

Имя	Тип	Размер
 Отсоединенная	Документ Microsoft Office Word	30 КБ
 Отсоединенная.docx	Файл "SIG"	<u>6 КБ</u>

Как добавить подпись



Чтобы к подписанному файлу добавить еще одну подпись, выберите файл с расширением *.SIG, отключите **Упрощенный режим** и выберите операцию **Добавить подпись**.



Примечание:
По количеству добавляемых подписей нет никаких ограничений.

Как добавить подпись



Проследуйте по шагам мастера добавления электронной подписи и выберите необходимые вам параметры и сертификат из личного хранилища.

КриптоАРМ :: Добавление ЭП

Параметры подписи
Установите желаемые параметры подписи

Свойства подписи

Использование подписи: [Не задано]

Комментарий к подписи:

Включить в подпись: Только сертификат владельца

Включить время создания подписи

Включить штамп времени на подписываемые данные

Включить штамп времени на подпись

Включить в подпись доказательства подлинности

< Назад Далее > Отмена

КриптоАРМ :: Добавление ЭП

Параметры подписи
Выберите сертификат для добавления подписи

Сертификат для создания подписи

Владелец сертификата:

Хеш алгоритм:

Выбрать Просмотреть

Отправить выходные файлы по электронной почте

Открыть окно почтового клиента

Выбор каталога сохранения выходных файлов

Поместить выходные файлы в указанный каталог

Выбор

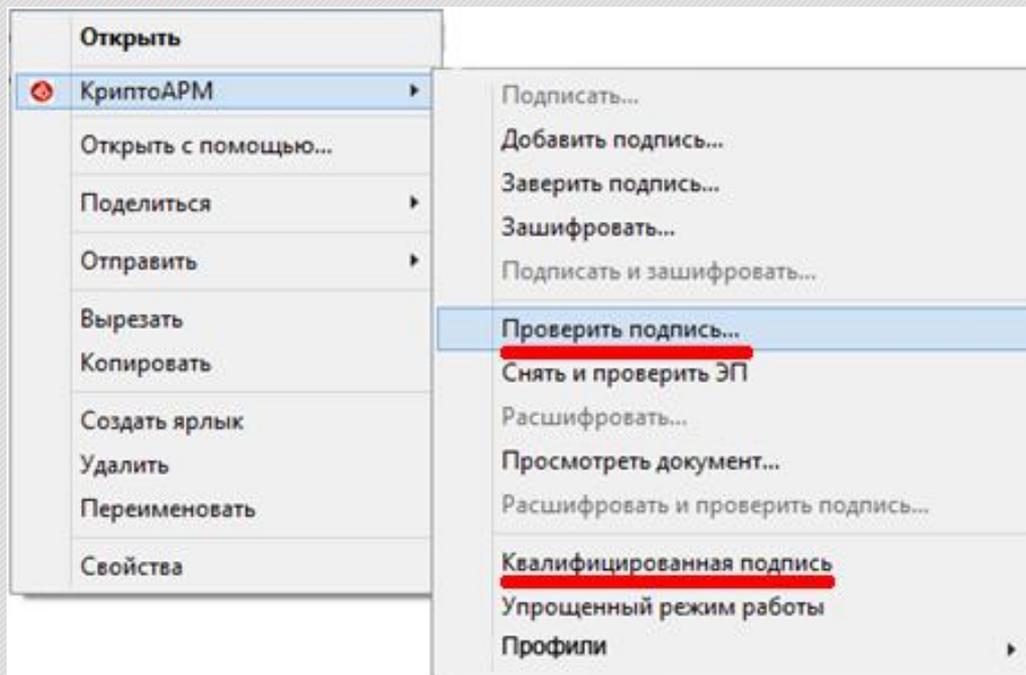
< Назад Далее > Отмена

Как проверить подпись



Чтобы проверить корректность электронной подписи, в контекстном меню файла выберите Проверить подпись.

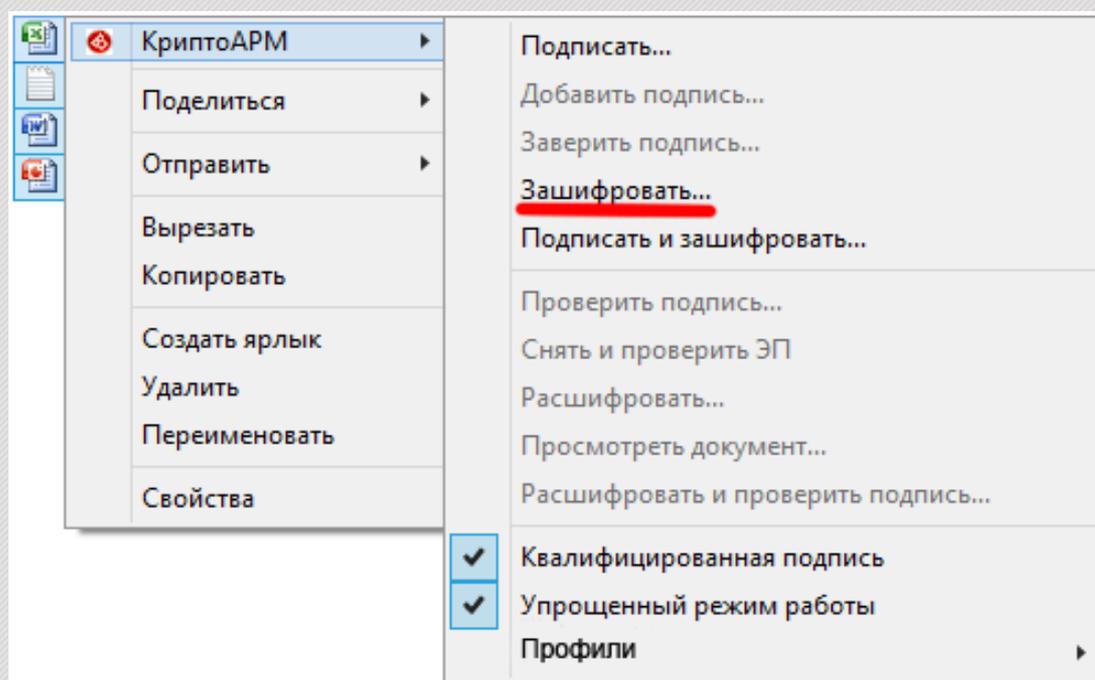
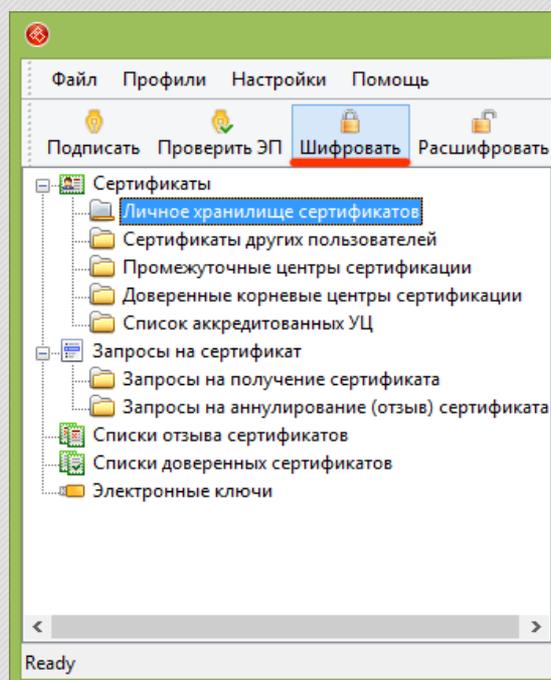
Если для вас важно проверить не только корректность электронной подписью, но и то, является ли она квалифицированной, убедитесь, что включен режим Квалифицированная подпись.



Как зашифровать файл



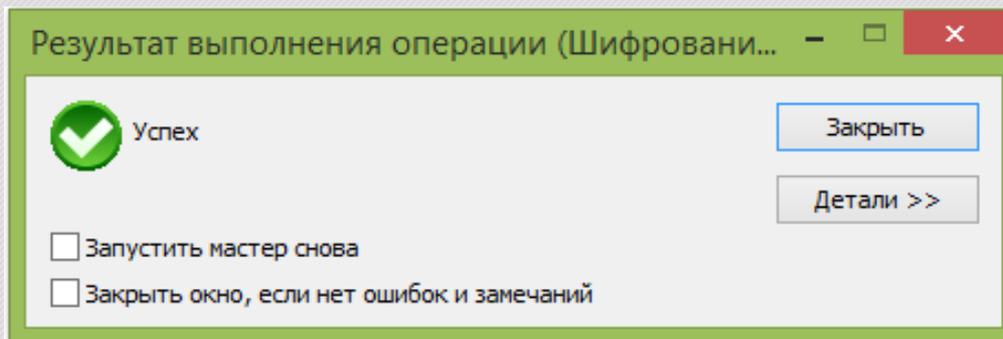
Зашифровать файлы можно в главном окне программы и через контекстное меню файла. Программа позволяет шифровать несколько файлов любого формата одновременно (в т.ч. файлы подписи).



Как зашифровать файл



В зависимости от размера и количества файлов, а также от конфигурации рабочего места операция может занять от нескольких секунд до нескольких минут.



Обратите внимание, что данное окно появится сразу только при использовании сохраненного профиля и упрощенного режима (см. страницы 18-22).

Как зашифровать файл



В результате операции в той же папке, в которой хранился исходный документ, появится файл с расширением *.ENC (шифрованные данные PKCS #7).

Обратите внимание, что файл, зашифрованный кодировкой «BASE-64», увеличивается в размере примерно на 40%.

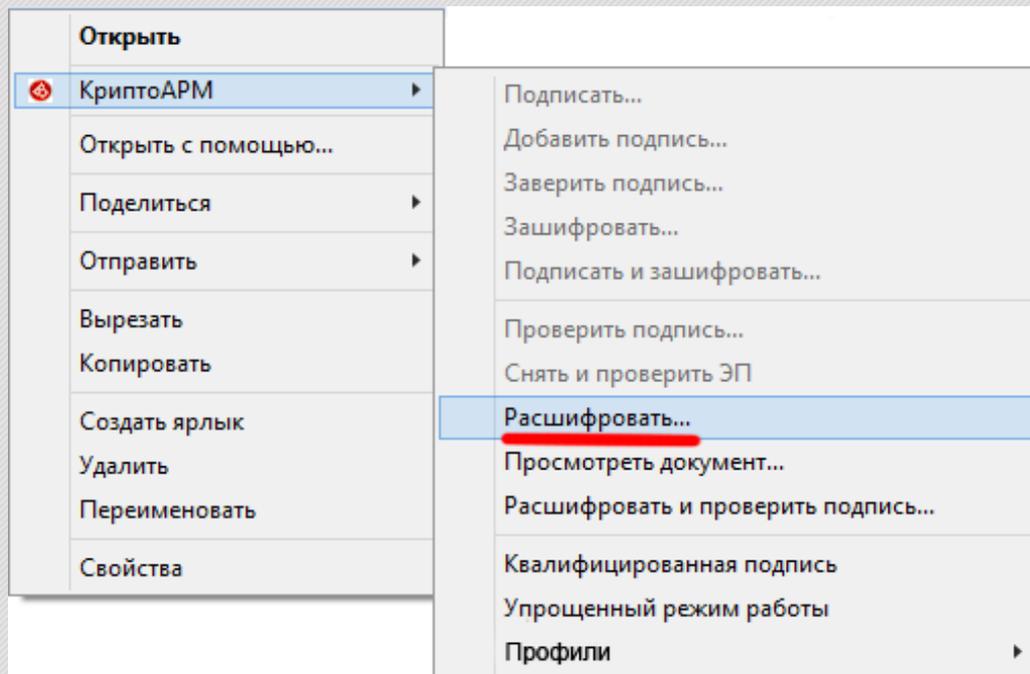
При сохранении кодировкой «DER» зашифрованный файл будет больше исходного на несколько килобайт (зависит от количества получателей зашифрованного файла).

Имя	Тип	Размер
 Шифрование	Adobe Acrobat Document	293 КБ
 Шифрование.pdf	Шифрованные данные PKCS #7	405 КБ

Как расшифровать файл



В контекстном меню файла выберите Расшифровать, и если ваш сертификат числится в списке получателей, то в текущем каталоге появится исходный (зашифрованный) документ.

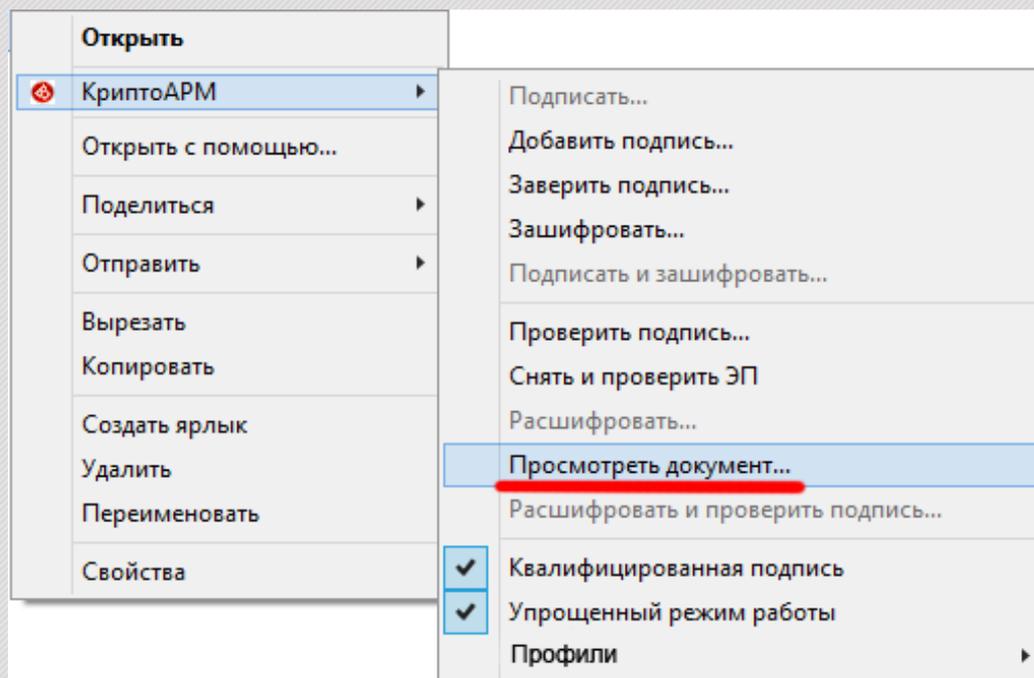


Как просмотреть документ



Если документ подписан отсоединенной подписью, то для просмотра документа достаточно открыть исходный файл.

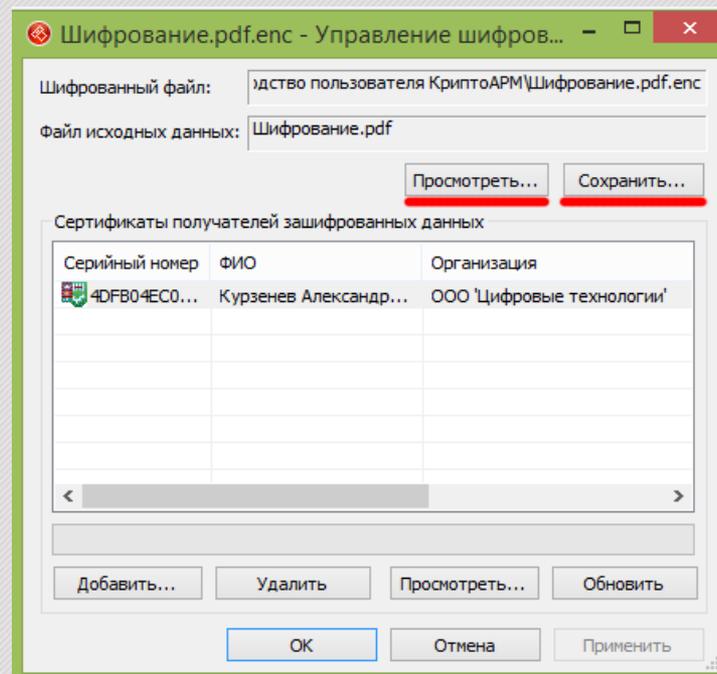
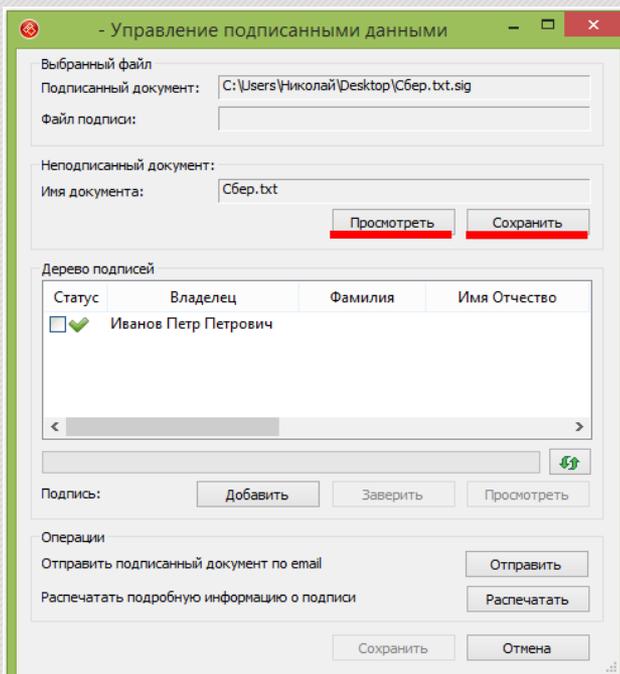
Если документ зашифрован или подписан совмещенной подписью, то просмотреть его можно одним из двух способов: через контекстное меню файла подписи (см. на картинке) или с помощью мастера управления подписанными и зашифрованными данными (см. далее).



Как просмотреть документ



Чтобы просмотреть исходный документ нажмите кнопку Просмотреть, чтобы сразу сохранить документ - Сохранить



Техническая поддержка



Если у вас появились вопросы, и вы не можете найти ответ в данном руководстве, обратитесь в техническую поддержку на нашем сайте.

